IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

TQP DEVELOPMENT, LLC,

Plaintiff

v.

(1) Ticketmaster Entertainment, Inc.;
(2) Fandango, Inc.;
(3) Apple Inc.;
(4) Live Nation, Inc.;
(5) Exxon Mobil Corporation;
(6) United Parcel Service, Inc.;
(7) CVS Caremark Corporation;
(8) DHL Express (USA), Inc.;
(9) MetLife, Inc.;
(10) Broadcast Music, Inc.;
(11) eBay Inc.;
(12) Half.com, Inc.;
(13) MicroPlace, Inc.;
(14) Viva Group, Inc.;
(15) ProStores, Inc.;
(16) PayPal, Inc.;
(17) Bill Me Later, Inc.;
(18) Comcast Corporation;
(19) Comcast Interactive Media, LLC;
(20) Plaxo, Inc.; and
(21) Exercise TV LLC.

Defendants.

Civil Action No. 2:09-cv-279

JURY TRIAL DEMANDED

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which TQP Development, LLC ("TQP") makes the following allegations against Ticketmaster Entertainment, Inc., Fandango, Inc., Apple Inc., Live Nation, Inc., Exxon Mobil Corporation, United Parcel Service, Inc., CVS Caremark Corporation, DHL Express (USA), Inc., MetLife, Inc., Broadcast Music, Inc., eBay Inc., Half.com, Inc., MicroPlace, Inc., Viva Group, Inc., ProStores, Inc., PayPal, Inc., Bill Me Later, Inc., Comcast Corporation, Comcast Interactive Media, LLC, Plaxo, Inc., and Exercise TV LLC (collectively the "Defendants").

PARTIES

1. Plaintiff TQP Development, LLC is a Texas limited liability company having a principal place of business of 207C North Washington Street, Marshall, Texas 75670.

2. On information and belief, Defendant Ticketmaster Entertainment, Inc. ("Ticketmaster") is a Delaware corporation with its principal place of business at 8800 Sunset Blvd., West Hollywood, CA 90069. Ticketmaster has appointed National Registered Agents, Inc. 160 Greentree Drive, Suite 101, Dover, DE 19904, as its agent for service of process.

3. On information and belief, Defendant Fandango, Inc. ("Fandango") is a Delaware corporation with its principal place of business at 12200 W. Olympic Blvd., Suite 150, Los Angeles, CA 90064. Fandango has appointed CT Corporation 818 W 7th St., Los Angeles, CA 90017-3425, as its agent for service of process.

4. On information and belief, Defendant Apple Inc. ("Apple") is a California corporation with its principal place of business at 1 Infinite Loop, Cupertino, CA 95014. Apple has appointed CT Corporation System, 350 N. St. Paul Street, Dallas, TX 75201, as its agent for service of process.

5. On information and belief, Defendant Live Nation, Inc. ("Live Nation") is a Delaware corporation with its principal place of business at 9348 Civic Center Dr., Beverly Hills, CA 90210. Live nation has appointed Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, DE 19808, as its agent for service of process.

6. On information and belief, Defendant Exxon Mobil Corporation ("Exxon") is a New Jersey corporation with its principal place of business at 5959 Las Colinas Blvd, Irving, TX 75039. Exxon has appointed Corporation Service Company, 830 Bear Tavern Road, West Trenton, NJ 08628, as its agent for service of process.

7. On information and belief, Defendant United Parcel Service, Inc. ("UPS") is a Delaware corporation with its principal place of business at 55 Glenlake Parkway, NE, Atlanta, GA 30328. UPS has appointed Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, DE 19808, as its agent for service of process.

8. On information and belief, Defendant CVS Caremark Corporation ("CVS") is a Delaware corporation with its principal place of business at 1 CVS Dr., Woonsocket, RI 02895. CVS has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

9. On information and belief, Defendant DHL Express (USA), Inc. ("DHL") is a Delaware corporation with its principal place of business at 1200 S. Pine Island Rd., Suite 600, Plantation, FL 33324. DHL has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

10. On information and belief, Defendant MetLife, Inc. ("MetLife") is a Delaware corporation with its principal place of business at 200 Park Ave., New York, NY 10166-0188. MetLife has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

11. On information and belief, Defendant Broadcast Music, Inc. ("Broadcast") is a New York corporation with its principal place of business at 320 W. 57th Street, New York, NY 10019-3790. Broadcast can be served at its physical address of 320 W. 57th Street, New York, NY 10019-3790.

12. On information and belief, Defendant eBay Inc. ("eBay") is a Delaware corporation with its principal place of business at 2145 Hamilton Ave., San Jose, CA 95125. eBay has appointed National Registered Agents, Inc., 160 Greentree Dr., Suite 101, Dover, DE 19904, as its agent for service of process.

13. On information and belief, Defendant Half.com, Inc. ("Half.com") is a Pennsylvania corporation with its principal place of business at 2145 Hamilton Avenue San Jose, CA 85125-5905. Half.com has appointed National Registered Agents, Inc., 1614 Sidney Baker Street, Kerrville, TX 78028-2640, as its agent for service of process.

14. On information and belief, Defendant MicroPlace, Inc. ("MicroPlace") is a Delaware corporation with its principal place of business at 2145 Hamilton Avenue, San Jose, CA 85125-5905. MicroPlace has appointed National Registered Agents, Inc., 2875 Michelle, Suite 100, Irvine, CA 92606-1024, as its agent for service of process.

15. On information and belief, Defendant Viva Group, Inc. ("Viva Group") is a Delaware corporation with its principal place of business at 2145 Hamilton Avenue, San Jose, CA 85125-5905. Viva Group has appointed National Registered Agents, Inc., 1821 Logan Avenue, Cheyenne, WY 82001-5007, as its agent for service of process.

16. On information and belief, Defendant ProStores, Inc. ("ProStores") is a Delaware corporation with its principal place of business at 2145 Hamilton Avenue, San Jose, CA 85125-5905. ProStores has appointed National Registered Agents, Inc., 2875 Michelle, Suite 100, Irvine, CA 92606-1024, as its agent for service of process.

17. On information and belief, Defendant PayPal, Inc. ("PayPal") is a Delaware corporation with its principal place of business at 2211 N. First St., San Jose, CA 95131. PayPal has appointed National Registered Agents, Inc., 160 Greentree Dr., Suite 101, Dover, DE 19904, as its agent for service of process.

18. On information and belief, Defendant Bill Me Later, Inc. ("Bill Me Later") is a Delaware corporation with its principal place of business at 2145 Hamilton Ave., San Jose, CA 95125. Bill Me Later has appointed National Registered Agents, Inc., 160 Greentree Dr., Suite 101, Dover, DE 19904, as its agent for service of process.

19. On information and belief, Defendant Comcast Corporation ("Comcast") is a Pennsylvania corporation with its principal place of business at One Comcast Center, Philadelphia, PA 19103-2838. On information and belief, Comcast has appointed Comcast Capital Corporation, 1201 N. Market Street, Suite 1000, Wilmington, Delaware 19801, as its agent for service of process.

20. On information and belief, Defendant Comcast Interactive Media, LLC ("Comcast Interactive") is a Delaware corporation with its principal place of business at One Comcast Center, Philadelphia, PA 19103-2838. Comcast Interactive has appointed Comcast Capital Corporation, 1201 N. Market Street, Suite 1000, Wilmington, Delaware 19801, as its agent for service of process.

21. On information and belief, Defendant Plaxo, Inc. ("Plaxo") is a Delaware corporation with its principal place of business at 203 Ravendale Drive, Mountain View, CA 94043. Plaxo has appointed Comcast Capital Corporation, 1201 N. Market Street, Suite 1000, Wilmington, Delaware 19801, as its agent for service of process.

22. On information and belief, Defendant Exercise TV LLC ("Exercise TV") is a Delaware corporation with its principal place of business at 11611 San Vicente Blvd., Suite 850, Los Angeles, CA 90049. Exercise TV has appointed Comcast Capital Corporation, 1201 N. Market Street, Suite 1000, Wilmington, Delaware 19801, as its agent for service of process.

JURISDICTION AND VENUE

23. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

24. Venue is proper in this district under 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, each Defendant has transacted business in this district, and has committed and/or induced acts of patent infringement in this district.

25. On information and belief, Defendants are subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to their substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 5,412,730

26. Plaintiff is the owner by assignment of United States Patent No. 5,412,730 ("the '730 Patent") entitled "Encrypted Data Transmission System Employing Means for Randomly Altering the Encryption Keys." The '730 Patent issued on May 2, 1995. A true and correct copy of the '730 Patent is attached as Exhibit A.

27. Upon information and belief, Defendant Ticketmaster has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, ticketmaster.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Ticketmaster and/or Ticketmaster's customers connect to Ticketmaster's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Ticketmaster's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Ticketmaster provides, or directs the client computer to provide, a seed value for both the transmitter and

receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Ticketmaster generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Ticketmaster encrypts data for transmission from the host server to the client. In addition, Ticketmaster directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Ticketmaster generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Ticketmaster decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Ticketmaster is thus liable for infringement of the ’730 Patent pursuant to 35 U.S.C. § 271.

28. Upon information and belief, Defendant Fandango has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ’730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on

various websites (including, without limitation to, fandango.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Fandango and/or Fandango's customers connect to Fandango's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Fandango's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Fandango provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Fandango generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Fandango encrypts data for transmission from the host server to the client. In addition, Fandango directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Fandango generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said

seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Fandango decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Fandango is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

29. Upon information and belief, Defendant Apple has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, store.apple.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Apple and/or Apple's customers connect to Apple's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Apple's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically

implements the claimed encryption algorithm under the direction of the host server. Apple provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Apple generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Apple encrypts data for transmission from the host server to the client. In addition, Apple directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Apple generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Apple decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Apple is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

30. Upon information and belief, Defendant Live Nation has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement

and/or contributing to the infringement of the ’730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, tickets.livenation.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ’730 Patent to the injury of TQP. For example, when Live Nation and/or Live Nation’s customers connect to Live Nation’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Live Nation’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Live Nation provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Live Nation generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Live Nation encrypts data for transmission from the host server to the client. In addition, Live Nation directs the client computer to encrypt data comprising information sent from the client to the host server before it

is transmitted over the link. Live Nation generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Live Nation decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Live Nation is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

31. Upon information and belief, Defendant Exxon has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, speedpass.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Exxon and/or Exxon's customers connect to Exxon's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with

encrypted portions of Exxon's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Exxon provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Exxon generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Exxon encrypts data for transmission from the host server to the client. In addition, Exxon directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Exxon generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Exxon decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Exxon is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

32. Upon information and belief, Defendant UPS has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, ups.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when UPS and/or UPS' customers connect to UPS' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of UPS' website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. UPS provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. UPS generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. UPS encrypts data for transmission from the host server to the client. In addition, UPS directs the client computer to

encrypt data comprising information sent from the client to the host server before it is transmitted over the link. UPS generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. UPS decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant UPS is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

33. Upon information and belief, Defendant CVS has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, cvs.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when CVS and/or CVS' customers connect to CVS' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer)

are encrypted according to the claimed method. In order to communicate with encrypted portions of CVS' website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. CVS provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. CVS generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. CVS encrypts data for transmission from the host server to the client. In addition, CVS directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. CVS generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. CVS decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for

example, a user of the client computer. Defendant CVS is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

34. Upon information and belief, Defendant DHL has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, sso.dhl-usa.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when DHL and/or DHL's customers connect to DHL's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of DHL's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. DHL provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. DHL generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a

predetermined characteristic of the data being transmitted over said link. DHL encrypts data for transmission from the host server to the client. In addition, DHL directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. DHL generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. DHL decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant DHL is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

35. Upon information and belief, Defendant MetLife has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, sisc.eservice.metlife.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when MetLife and/or MetLife's customers connect to MetLife's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a

sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of MetLife's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. MetLife provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. MetLife generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. MetLife encrypts data for transmission from the host server to the client. In addition, MetLife directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. MetLife generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. MetLife decrypts data sent from the client in order to use the data,

and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant MetLife is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

36. Upon information and belief, Defendant Broadcast has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, bmi.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Broadcast and/or Broadcast's customers connect to Broadcast's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Broadcast's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Broadcast provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Broadcast generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer

is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Broadcast encrypts data for transmission from the host server to the client. In addition, Broadcast directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Broadcast generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Broadcast decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Broadcast is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

37. Upon information and belief, Defendant eBay has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, signin.ebay.com, signin.half.ebay.com, microplace.com, rent.com, mystore.prostores.com, and billmelater.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when eBay and/or eBay's

customers connect to eBay's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of eBay's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. eBay provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. eBay generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. eBay encrypts data for transmission from the host server to the client. In addition, eBay directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. eBay generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being

produced each time a predetermined number of said blocks are transmitted over said link. eBay decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant eBay is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

38. Upon information and belief, Defendant Half.com has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, signin.half.ebay.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Half.com and/or Half.com's customers connect to Half.com's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Half.com's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Half.com provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Half.com generates, or directs the

client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Half.com encrypts data for transmission from the host server to the client. In addition, Half.com directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Half.com generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Half.com decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Half.com is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

39. Upon information and belief, Defendant MicroPlace has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, microplace.com) for transmitting data

comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ’730 Patent to the injury of TQP. For example, when MicroPlace and/or MicroPlace’s customers connect to MicroPlace’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of MicroPlace’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. MicroPlace provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. MicroPlace generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. MicroPlace encrypts data for transmission from the host server to the client. In addition, MicroPlace directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. MicroPlace generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence

being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. MicroPlace decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant MicroPlace is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

40. Upon information and belief, Defendant Viva Group has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, rent.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Viva Group and/or Viva Group's customers connect to Viva Group's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Viva Group's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction

of the host server. Viva Group provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Viva Group generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Viva Group encrypts data for transmission from the host server to the client. In addition, Viva Group directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Viva Group generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Viva Group decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Viva Group is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

41. Upon information and belief, Defendant ProStores has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement

and/or contributing to the infringement of the ’730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, mystore.prostores.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ’730 Patent to the injury of TQP. For example, when ProStores and/or ProStores’ customers connect to ProStores’ website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of ProStores’ website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. ProStores provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. ProStores generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. ProStores encrypts data for transmission from the host server to the client. In addition, ProStores directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link.

ProStores generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. ProStores decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant ProStores is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

42. Upon information and belief, Defendant PayPal has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to billmelater.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when PayPal and/or PayPal's customers connect to PayPal's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with

encrypted portions of PayPal's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. PayPal provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. PayPal generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. PayPal encrypts data for transmission from the host server to the client. In addition, PayPal directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. PayPal generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. PayPal decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant PayPal is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

43. Upon information and belief, Defendant Bill Me Later has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ’730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, billmelater.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ’730 Patent to the injury of TQP. For example, when Bill Me Later and/or Bill Me Later’s customers connect to Bill Me Later’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Bill Me Later’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Bill Me Later provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Bill Me Later generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Bill Me Later encrypts

data for transmission from the host server to the client. In addition, Bill Me Later directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Bill Me Later generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Bill Me Later decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Bill Me Later is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

44. Upon information and belief, Defendant Comcast has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, comcast.com, login.comcast.net, plaxo.com, fandango.com and store.exercisetv.tv) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Comcast and/or Comcast's customers connect to Comcast's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is

transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Comcast's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Comcast provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Comcast generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Comcast encrypts data for transmission from the host server to the client. In addition, Comcast directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Comcast generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Comcast decrypts data sent from the client in order to use the data, and directs the

client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Comcast is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

45. Upon information and belief, Defendant Comcast Interactive has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, login.comcast.net) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Comcast Interactive and/or Comcast Interactive's customers connect to Comcast Interactive's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Comcast Interactive's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Comcast Interactive provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Comcast Interactive generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on

said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Comcast Interactive encrypts data for transmission from the host server to the client. In addition, Comcast Interactive directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Comcast Interactive generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Comcast Interactive decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Comcast Interactive is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

46. Upon information and belief, Defendant Plaxo has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, plaxo.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims

of the ‘730 Patent to the injury of TQP. For example, when Plaxo and/or Plaxo’s customers connect to Plaxo’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Plaxo’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Plaxo provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Plaxo generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Plaxo encrypts data for transmission from the host server to the client. In addition, Plaxo directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Plaxo generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in

a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Plaxo decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Plaxo is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

47. Upon information and belief, Defendant Exercise TV LLC has been and now is directly and jointly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United Stated, by, among other things, methods practiced on various websites (including, without limitation to, store.exercisetv.tv) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Exercise TV LLC and/or Exercise TV LLC's customers connect to Exercise TV LLC's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Exercise TV LLC's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Exercise TV LLC provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a

symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Exercise TV LLC generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Exercise TV LLC encrypts data for transmission from the host server to the client. In addition, Exercise TV LLC directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Exercise TV LLC generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Exercise TV LLC decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Exercise TV LLC is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

48. On information and belief, to the extent any marking was required by 35 U.S.C. § 287, all predecessors in interest to the '730 Patent complied with any such requirements.

49. To the extent that facts learned in discovery show that Defendants' infringement of the '730 Patent is or has been willful, Plaintiff reserves the right to request such a finding at time of trial.

50. As a result of these Defendants' infringement of the '730 Patent, Plaintiff has suffered monetary damages and is entitled to a money judgment in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants, together with interest and costs as fixed by the court, and Plaintiff will continue to suffer damages in the future unless Defendants' infringing activities are enjoined by this Court.

51. Unless a permanent injunction is issued enjoining these Defendants and their agents, servants, employees, representatives, affiliates, and all others acting on in active concert therewith from infringing the '730 Patent, Plaintiff will be greatly and irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

1. A judgment in favor of Plaintiff that Defendants have infringed, directly, jointly, and/or indirectly, by way of inducing and/or contributing to the infringement of the '730 Patent, and that such infringement was willful;

2. A permanent injunction enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert therewith from infringement, inducing the infringement of, or contributing to the infringement of the '730 Patent;

3. A judgment and order requiring Defendants to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for Defendants' infringement of the '730 Patent as provided under 35 U.S.C. § 284;

4. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees; and

5. Any and all other relief to which Plaintiff may show itself to be entitled.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Respectfully submitted,

Dated: October 13, 2009

By: /s/ *Marc A. Fenster*
Marc A. Fenster, CA Bar No. 181067
E-mail: mfenster@raklaw.com
RUSS, AUGUST & KABAT
12424 Wilshire Boulevard 12th Floor
Los Angeles, California 90025
Telephone: 310/826-7474
Facsimile: 310/826-6991

Harold Kip Glasscock, Jr.- LEAD COUNSEL
TX Bar # 08011000
E-mail: kipglasscock@hotmail.com
KIP GLASSCOCK, P.C.
550 Fannin, Suite 1350
Beaumont, Texas 77701
Telephone: 409/833-8822
Facsimile: 409/838-4666

John M. Bustamante, TX Bar # 24040618
Email: jmb@bustamantelegal.com
BUSTAMANTE PC
54 Rainey Street, No. 721
Austin, Texas 78701
Telephone: 512/940-3753
Facsimile: 512/551-3777

Attorneys for Plaintiff
TQP DEVELOPMENT, LLC

CERTIFICATE OF SERVICE

I hereby certify that the counsel of record who are deemed to have consented to electronic service are being served on October 13, 2009 with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3). Any other counsel of record will be served by electronic mail, facsimile transmission and/or first class mail on this same date.

October 13, 2009 By: /s/ *Marc A. Fenster*
Marc A. Fenster